

EXHIBIT D:

PhoneFactor Infringement Claim Chart

Reference Documents

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 1 – PhoneFactor Functional Diagram (From Remote Access VPNs datasheet)

Section 2 – PhoneFactor Remote Access VPNs Datasheet

<http://www.phonefactor.com/solutions/ssl-vpn-authentication>

Section 3 – PhoneFactor Standard Edition Datasheet

<http://www.phonefactor.com/products/phonefactor-standard>

Section 4 – PhoneFactor Home Page

<http://www.phonefactor.com/>

Section 5 – The Authentication Revolution: Phones Become the Leading Multi-Factor Authentication Device. PhoneFactor Whitepaper

Section 6 – PhoneFactor: Phone-Based Two-Factor Authentication. PhoneFactor Whitepaper

Section 7 – PhoneFactor SMS (Text) Authentication Datasheet

<http://www.phonefactor.com/products/sms-text-authentication>

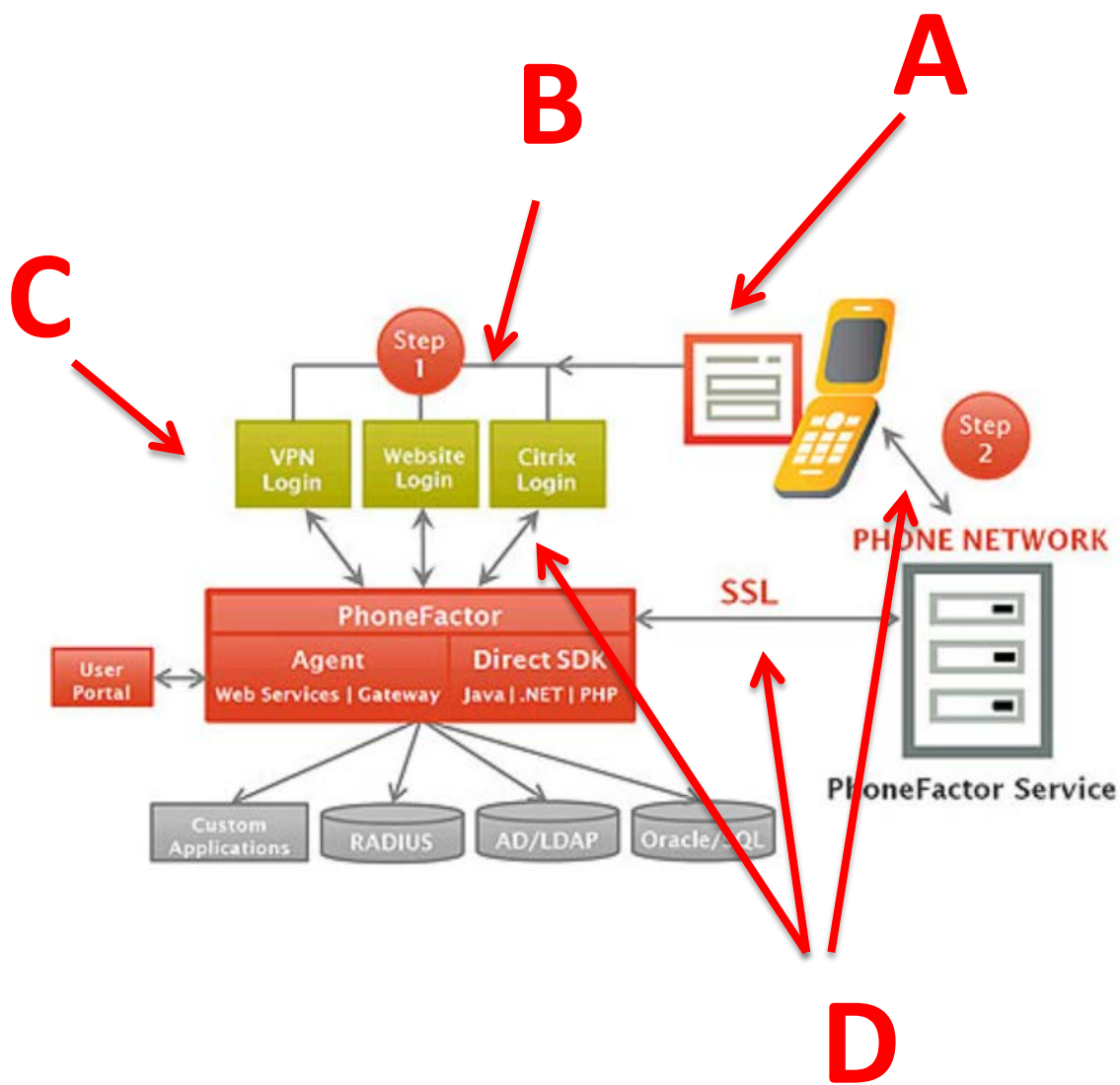
Section 8 – Comparing PhoneFactor to Other SMS Authentication Solutions Datasheet

<http://www.phonefactor.com/sms-authentication>

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 1

PhoneFactor Functional Diagram (From
Remote Access VPNs datasheet)



D1, D2, D3

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 2

PhoneFactor Remote Access VPNs Datasheet

<http://www.phonefactor.com/solutions/ssl-vpn-authentication>

**PhoneFactor**[Free Download](#)[Resource Center](#)[Customer Login](#)**1.877.No.Token** (1.877.668.6536)[Live Chat](#)[Online Demo](#)[Free Download](#)[Solutions](#)[Products](#)[How It Works](#)[Company](#)

Remote Access VPNs

Remote Access Authentication Solutions

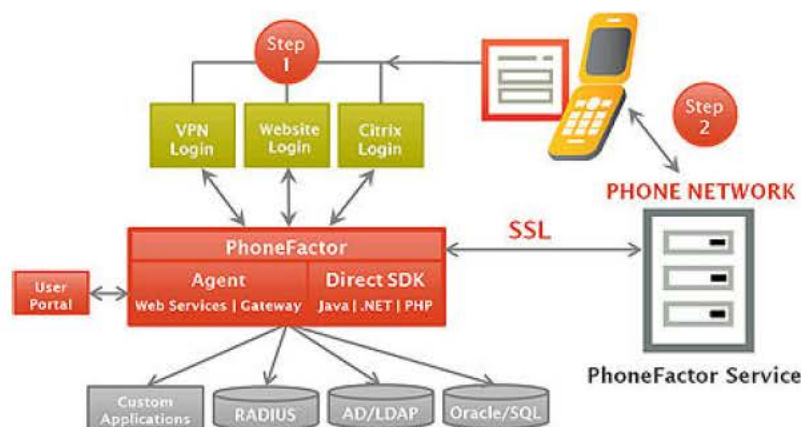
Secure access to your Virtual Private Network (VPN) in minutes with PhoneFactor.

- RADIUS plug-in for easy set up and no new hardware to install
- No tokens, software or certificates to deploy and manage
- Authentication via a phone call, sms text message, or phone app
- Out-of-band authentication offers enhanced security

How It Works

PhoneFactor can be seamlessly integrated with all leading VPN appliances using RADIUS. When a user logs into their company's VPN, a RADIUS request is made to the PhoneFactor Agent, which acts as a RADIUS proxy server. It first validates the user name and password with the target RADIUS server before initiating a PhoneFactor authentication.

PhoneFactor's hybrid service architecture allows organizations to store all critical user data within their infrastructure while leveraging the high-scale PhoneFactor Service to place authentication calls, send text messages, and communicate with the PhoneFactor App. The PhoneFactor Service is supported by a network of redundant data centers and telecommunications providers ensuring the highest level of availability.



Download

[Download PhoneFactor](#) to authenticate up to 25 users for free. Then upgrade at any time to enable additional users or take advantage of advanced features, including:

- Agent Redundancy and Load Balancing
- Active Directory and LDAP Integration
- Real-Time Fraud Alerts
- User Self-Enrollment Capabilities
- User Management Tools for Help Desks
- Enhanced Logging and Reporting Capabilities
- Custom Greetings and Caller ID
- Biometric Voice Authentication

**Demo PhoneFactor**

See for yourself
how easy it is.

**Get PhoneFactor****It's Free**

Sign up now to get started.

**Contact Us****Call 877.No.Token****Or click to [Chat Live](#)**

Solutions

By Industry

- Enterprise
- Government
- Banking & Finance
- Healthcare
- eCommerce

By Application

- Remote Access VPNs
- Websites & Web Mail
- Cloud Services
- Online Banking
- Citrix
- IBM Tivoli
- Terminal Services
- Imprivata
- LogMeIn
- Regulatory Compliance



PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 3

PhoneFactor Standard Edition Datasheet

<http://www.phonefactor.com/products/phonefactor-standard>



PhoneFactor

[Free Download](#)
[Resource Center](#)
[Customer Login](#)
1.877.No.Token (1.877.668.6536)

[Live Chat](#)
[Online Demo](#)
[Free Download](#)
[Solutions](#)
[Products](#)
[How It Works](#)
[Company](#)

PhoneFactor Standard

The PhoneFactor Standard Edition is a robust platform for authenticating enterprise and website logins.

The Standard Edition:

- Offers a Choice Between Phone Call and Text Message Methods
- Adds Out-Of-Band Authentication for Up To Two Applications
- Enables PIN Security for a Third Layer of Protection
- Sends Real-Time Alerts of Fraudulent Activity
- Provides Centralized Reporting for Auditing/Compliance
- Ensures High Availability with Agent Redundancy and Fail Over
- Configures for Leading Applications in Minutes
- Seamlessly Integrates with Existing Websites and Transactions

Key Features

PIN Security

Add a third layer of protection by requiring users to enter a personal identification number (PIN) to authenticate. Administrators control which users are enabled for PIN security and set rules to enforce PIN strength and expiration policies.

Real-Time Fraud Alerts

Receive instant notification if users suspect fraudulent activity on their account. Users simply choose the fraud alert option during the authentication, blocking access to their account and triggering an e-mail to your IT team.

Application Integration

PhoneFactor offers out-of-the-box integration with VPNs, Outlook Web Access, Citrix Web Interface, Terminal Services, IIS websites, and any RADIUS application. A wizard simplifies the configuration process, which takes just minutes. Secure up to two applications with the Standard Edition.

User Import

Import users from your existing Active Directory or any CSV file. Instantly enable users with phone numbers and send them an automated welcome e-mail.

Fail Over Protection and Load-Balancing

Real-time synchronization between two fully functional PhoneFactor agents allows for a primary and backup server or operation of redundant web servers.

Customized User Experience

Customize the PhoneFactor experience for your users. Increase usability with phone prompts specific to your company and home language, identify the authentication call as originating from your company, and customize the automated welcome e-mail that is sent to users.

Advanced Calling Options

PhoneFactor can reach users wherever they are with support for direct dial to any home, cell, or work number as well as corporate phone menus for users with extensions. If a user can't be reached at their primary number, the system can automatically dial the user's alternate phone number.

User Phone and PIN Management

Users can manage their own phone and PIN changes from the phone menu during an authentication call. If the user's PIN has expired, they will be prompted to enter a new PIN to complete the authentication.


Demo PhoneFactor

See for yourself
how easy it is.


Get PhoneFactor
It's Free

Sign up now to get started.


Contact Us

Call **877.No.Token**

Or click to **Chat Live**

Products

PhoneFactor Free

PhoneFactor Standard

PhoneFactor Extended

SMS Text Authentication

Biometric Authentication

Transaction Verification

Phone Verification

Global Services


24/7 Support

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents



Section 4

PhoneFactor Home Page


<http://www.phonefactor.com/>



B
A

[Free Download](#) | [Resource Center](#) | [Customer Login](#)
1.877.No.Token () **1.877.668.6536** )
[Live Chat](#)

[Online Demo](#) | [Free Download](#) | [Solutions](#) | [Products](#) | [How It Works](#) | [Company](#)



BECAUSE PASSWORDS JUST AREN'T ENOUGH

Get the **multi-factor authentication** you need to protect against today's threats without the hassle and cost of yesterday's technology.

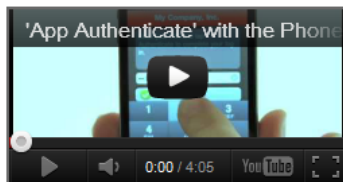
- Easy to set up, manage, and use
- Strong out-of-band authentication
- Phone call, text, and phone app options
- Far less expensive than tokens

[Demo](#)
[Free Download](#)

Secure Authentication for: [Enterprises](#) [Government](#) [Healthcare](#) [Banking & Finance](#) [eCommerce](#)

Introducing...

Meet the latest addition to PhoneFactor's out-of-band authentication platform - the phone app.



The Authentication Revolution

Over the last few years, phone-based authentication has displaced legacy systems as the authentication method of choice. [Download this whitepaper](#) to find out why.



PhoneFactor vs Security Tokens

PhoneFactor offers a number of benefits over security tokens, including:

- Decreased Risk of a Breach
 - 100% Out-of-Band Security
 - Instant Fraud Alerts
 - Biometric Voice Authentication
 - Transaction Verification
- Superior User Experience
- No Extra Devices to Carry
 - No End User Training Required

- Reduced Deployment and Mgmt Time
- No Devices to Buy, Ship, Replace or Renew
 - Automated User Enrollment
 - Reduced Help Desk Calls

Significant Cost Savings

> [Learn More](#)



Updated Authentication Guidance Calls for Stronger Security and Compliance by January 2012

The latest FFIEC Guidance requires banks to employ a layered approach and stronger authentication, such as out-of-band methods, to protect financial institutions and their customers from online banking fraud.

Find out how PhoneFactor's out-of-band platform, featuring user authentication and transaction verification capabilities, can enable compliance before your next bank exam.

> [Download Whitepaper](#)

> [View Webcast](#)

> [Visit Resource Center](#)

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 5

**“The Authentication Revolution: Phones
Become the Leading Multi-Factor
Authentication Device”**

PhoneFactor Whitepaper

The Authentication Revolution: Phones Become the Leading Multi-Factor Authentication Device



PhoneFactor, Inc.
7301 West 129th Street
Overland Park, KS 66213
1-877-668-6536
www.phonefactor.com

Executive Summary

Escalating IT security threats and strengthening regulatory requirements are driving adoption of multi-factor authentication to unprecedented levels. Increasingly, new and expanded multi-factor implementations are leveraging phone-based authentication instead of security tokens, which had previously dominated the multi-factor market. According to Goode Intelligence, an information security research and analysis firm, phone-based authentication will comprise 61% of the multi-factor authentication market by the year 2014.

This paper will address the key drivers for this market shift and includes real-world case studies from organizations that have made the move to phone-based authentication. It also introduces PhoneFactor, the leading provider of phone-based multi-factor authentication.

Contents

What Is Phone-Based Multi-Factor Authentication?	3
Phone-Based Authentication Becomes The Method of Choice	4
User Adoption	4
Security	4
Scalability	5
PhoneFactor Overview	5
How PhoneFactor Works	6
Scalable Architecture	7
Seamless Integration	7
Rapid Deployment & Minimal Support	7
Case Studies	8
OhioHealth – Large Regional Healthcare Organization	8
Regis - World's Largest Operator of Hair Salons	9
Proven Success & Industry Leadership	10

What Is Phone-Based Multi-Factor Authentication?

Authentication, which is the process by which a computer system positively identifies a user, is considered to be one of the weakest links in computer security today. Every day a new story emerges about a computer breach or incident of online fraud resulting from compromised credentials. With the proliferation of remote access and cloud computing among enterprises and increased use of e-commerce and online banking, the trend is only going to continue. Authentication systems that rely solely on user names and passwords are subject to a number of vulnerabilities, including notoriously poor user password choices, password harvesting via key logging software, phishing and man-in-the-middle attacks, and others.

Multi-factor authentication adds a critical second layer of security to user logins and transactions. It works by requiring any two or more of the following:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated)
- Something you are (biometrics)

The security of multi-factor authentication lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the trusted device. Conversely, if the user happens to lose the device, the finder of that device won't be able to use it unless he or she also knows the user's password.

Until recently, the predominant multi-factor authentication system has been security tokens, like RSA's SecurID. Security tokens rely on a hardware token that generates a One-Time-Passcode (OTP). The user is required to enter the OTP into the login screen to verify that they have possession of the trusted device. While security tokens provide an additional level of security over single-factor authentication, they have proven to be cumbersome for IT departments and end users. In addition, more sophisticated threats have emerged that defeat security tokens.

Phone-based authentication systems leverage the user's telephone as the trusted device for the second factor or authentication. Telephones are extremely difficult to duplicate and phone numbers are extremely difficult to

intercept. The combination of the phone and a username/password yields strong, multi-factor authentication with minimal impact on the user experience.

Phone-Based Authentication Becomes the Method of Choice

Leveraging a ubiquitous device to secure logins and transactions provides a number of benefits for end users and IT departments.

User Adoption

The phone is an inherently user-friendly device and is accessible for users with disabilities. Everyone knows how to use a phone, so no end user training is required.

Cell phones have become a critical part of everyday life for the vast majority of people in all demographic groups. People can't go to a different part of their house without taking their cell phone with them. Since users already carry a phone, using the device for authentication is a natural extension of its capabilities. Users don't want to carry around one more thing or have another item dangling from their keychain. Security tokens and other two-factor devices are easily lost or forgotten by users.

Users want the freedom to login from any device, including home PCs, laptops and mobile phones, and to login from any location, including internet cafes, airport WI-FIs, remote offices, and client sites. The variety of devices and connection points can present significant challenges for IT departments, but the need for this level of portability by users will only increase going forward. Phone-based authentication affords this level of flexibility. The same phone can be used to authenticate any application, eliminating the need for multiple devices, and works anywhere in the world. If a user loses or damages his or her phone, a replacement device can be purchased from a local retailer.

Security

Increasingly, out-of-band methods that complete the second factor of authentication through a separate and unique channel are becoming a security best practice. Out-of-band authentication is critical to protect against man-in-the-middle and man-in-the-browser attacks which defeat security tokens.

The telephone network provides an ideal second channel for authenticating users. As a two-way, active communications channel, important information, such as transaction details, can be relayed to the user and the user can verify the login or provide input, such as a confirmation code, through the telephone. While some phone-based authentication methods work like a security token by generating an OTP that is keyed into the login interface for an in-band authentication process, others, like PhoneFactor are completely out-of-band.

This open communication channel also allows for seamless verification of a third factor of authentication. The user's voiceprint can be matched during an authentication call enabling biometric authentication without requiring special hardware, like a fingerprint scanner.

Scalability

Since security tokens must be provisioned, mailed, inventoried, and replaced, they require significant IT resources to deploy and support. Security tokens are lost at a rate of up to 10% each year, expiring tokens must be re-provisioned every 2-5 years, and tokens can get out of sync. The resulting costs to an IT department can become a material part of the total cost of ownership for a token solution.

With phone-based authentication, there are no devices to deploy. It can be quickly enabled for large numbers of geographically diverse users and is cost-effective to set up and maintain.

These factors (user adoption, security, and scalability) represent the primary drivers for adoption of phone-based authentication and address inherent weaknesses in authentication systems based on security tokens. As this market shift has accelerated over the last few years, PhoneFactor's phone-based multi-factor authentication system has assumed a leadership position in terms of both the strength of its technology and market adoption. According to Goode Intelligence, "this technology [voice-based authentication] is dominated by one technology vendor, PhoneFactor."

PhoneFactor Overview

PhoneFactor's strong, out-of-band authentication offers a robust, scalable platform for internal and customer-facing applications. With PhoneFactor, users can choose the authentication method they prefer - phone call, text message, or phone app - all with the same level of out-of-band security

and convenience. Additional security features, like PIN mode, voiceprint, and transaction verification, can be mapped to particular users and/or levels of risk.

Phone Call: PhoneFactor confirms possession of a trusted device - the user's phone - through an automated phone call. The user answers the call and presses # to authenticate.

Text Message: PhoneFactor sends a text message containing a one-time passcode to the user. The user replies to the text message with the passcode to authenticate.

App: PhoneFactor pushes a notification to the PhoneFactor App on the user's smart phone or tablet. The user taps "Authenticate" in the app to authenticate.

PIN Security & Voiceprint: By requiring the user to also verify a secret PIN, PhoneFactor can further ensure that the user has possession of the telephone at the time of the authentication. For three-factor authentication, the user speaks a secret passphrase during the phone call to also verify his or her voiceprint. Advanced voice biometric technology ensures accurate, reliable voiceprint verification.

Transaction Verification: For high-risk and high-value transactions, such as ACH and wire transfers, details about the transaction can be provided as part of the authentication request. The user can then approve or deny that specific transaction.

Fraud Alerts: If a user receives an authentication request from PhoneFactor for a login or transaction he or she did not initiate, the user can simply enter 911# during the call or in a text message response or tap "Deny and Report Fraud" in the phone app. This locks the account and instantly alerts the company's fraud department that the user's credentials have been compromised and an attack is in progress.

How PhoneFactor Works

In addition to a rich set of features, PhoneFactor offers a highly-scalable service architecture, a number of off-the-shelf integration options, and self-enrollment and management tools. As a result, PhoneFactor set up is easy, deployment to end users is quick, and ongoing maintenance is minimal.

Scalable Architecture

PhoneFactor adds a second step to existing authentication processes. If the username and password are correct, an SSL request is sent to the PhoneFactor Service, which is housed in one of PhoneFactor's data centers around the world. The PhoneFactor Service places an automated phone call, sends a text message, or pushes a notification the PhoneFactor App on the user's mobile device and processes the results. Finally, it returns success or failure to the application. The PhoneFactor Service is supported by a network of redundant data centers and telecommunications providers ensuring the highest level of availability.

Seamless Integration

PhoneFactor offers instant integration with a wide range of applications, including all leading remote access VPN solutions, single sign-on systems, cloud applications, online banking, and websites as well as custom applications. A number of integration options enable rapid implementation and maximum flexibility, including:

- Built-in support for Citrix, Tivoli, Cisco VPNs, Outlook Web Access, Terminal Services and IIS websites among others
- Web plug-ins for Java, .Net, PHP, Perl, and Ruby or a web services SDK
- Universal Web Gateway, which adds an authentication layer to any website without requiring that the website be modified

Rapid Deployment & Minimal Ongoing Support

PhoneFactor offers self-enrollment and management tools to streamline user deployment and support. Organizations can leverage existing directory system(s) to auto-enable new users and update existing users. Enrolling users is as simple as 1-2-3:

Step 1: Users are imported from AD/LDAP.

Step 2: Users receive an email from PhoneFactor with a link to the User Portal (a simple web interface hosted within your network) to enroll.

Step 3: Users click the link, specify a phone number and security questions, and complete a test authentication. PhoneFactor App users will also be provided with an activation code that is entered into the app on their smart phone or tablet.

That's it. The next time the user logs into a PhoneFactor secured application, he or she will receive an authentication request from PhoneFactor. No further user training is required.

The user can manage his or her phone number(s) and PIN by returning to the User Portal or during any authentication call. Administrative capabilities are also available through the User Portal to enable help desk staff to provide user support.

Emergency access can be enabled in the rare case where the user cannot be reached at his or her registered phone number(s) by creating a one-time bypass in the User Portal.

Case Studies: Leading Companies Move to Phone-Based Authentication to Increase Security & Decrease Costs

OhioHealth – Large Regional Healthcare Organization

The Business Challenge: OhioHealth is a nationally recognized, not-for-profit healthcare organization serving and supporting Ohio's healthcare needs. Based in Columbus, OhioHealth is a family of 15 hospitals, 20 health and surgery centers, home-health providers, medical equipment and health service suppliers. OhioHealth employs more than 14,000 healthcare professionals.

OhioHealth was looking for a two-factor solution to replace 4,300 RSA tokens which were proving to be high in cost and maintenance. Training new users and replacing each token was a major task. In addition to these management hassles, doctors on staff with several hospitals were required to carry multiple tokens.

The Solution: PhoneFactor's phone-based approach was selected over RSA SecurID tokens for its ability to eliminate implementation and maintenance hassles, provide ease of use, and significantly lower overall cost. The benefits included:

- **Consistency in the User Workflow:** There was no cumbersome hardware installation/transition and no hard "change-over" date for users. Users were simply transitioned as tokens expired.
- **Streamlined User Provisioning and Management:** OhioHealth has deployed the PhoneFactor User Portal to enable users to complete their own enrollment, and integrated PhoneFactor with their existing Active Directory for streamlined user provisioning and management. An automated email trains new users on the system.
- **Regulatory Compliance:** Since the initial roll out, OhioHealth expanded their PhoneFactor implementation to address two-factor requirements by the Ohio Pharmacy Board.

- Increased Efficiency: Physicians and staff members spend less time dealing with authentication “headaches” allowing them to focus on their first priority, their patients.
- Cost Savings: OhioHealth realized significant savings on both initial and ongoing hard and soft costs.

“We decided to switch to PhoneFactor’s two-factor solution from tokens because it’s a ‘one and done’ solution. It’s simple to use and simple for the help desk to add a new member or adjust the information for a lost cell phone. PhoneFactor requires fewer resources, reduced management overhead and overall improved customer satisfaction.” - Jim Lowder, Vice President, Technology for OhioHealth.

Regis Corporation - World’s Largest Operator of Hair Salons

The Business Challenge: With more than 12,000 locations worldwide, remote access security across the Regis network is no small job. Two-factor authentication for remote access was critical to meet Regis’ own rigorous security policies, but was also a requirement to maintain compliance with industry regulations such as the Payment Card Industry Data Security Standards (PCI DSS). They had previously used RSA tokens and neither employees nor the IT staff was happy with that solution. They needed a solution that was easier for everyone, and that also met the PCI standards.

The Solution: Before choosing PhoneFactor, Regis had struggled with the difficulty of using tokens and other two-factor methods. Their non-technical users found these solutions challenging and the IT department was spending far too much time supporting them. Regis wanted a turnkey solution for remote access that would be easy for their non-technical users to manage and minimize back-end support needs.

Using PhoneFactor has affected the way business operates at Regis. In fact, Regis notes numerous benefits by switching to PhoneFactor’s two-factor solution:

- Decreased Deployment Timeframe: Regis rolled out PhoneFactor quickly, first as a pilot and then through their normal ongoing cycle of hardware and software updates.
- Increased User Response/Adoption: Regis users found PhoneFactor to be much more convenient than fob-based tokens. It was so easy that they trained their staff via memo only.

- Ongoing Reduced Costs: With PhoneFactor, there is virtually no maintenance for the IT staff at Regis, significantly reducing their total cost of ownership.
- Increased Security/Compliance: PhoneFactor filled the PCI DSS requirement for two-factor authentication. In addition, PhoneFactor's instant fraud alerts were incorporated into Regis' official incident response plan.
- Easy Expansion: PhoneFactor makes roll-out to additional users simple.

"It's no-hassle security, and has reduced the complaints to the Help Desk about access issues. It has worked just as we hoped and was an easy transition." - Joel Wiens, Vice President of Information Technology, Regis Corporation

Proven Success & Industry Leadership

PhoneFactor combines strong out-of-band security with unparalleled ease of use for both users and IT departments, ultimately reducing the risk of a data breach at a lower total cost of ownership. As companies increasingly look to phone-based authentication to address today's threats while also meeting the needs of growing numbers of enterprise and consumer users, PhoneFactor is the leading choice. PhoneFactor is trusted by thousands of organizations across virtually every industry, including Retail, Government, Healthcare, and Banking, to secure millions of logins and online transactions each month.

PhoneFactor was recognized in 2011, 2010, and 2008 as an SC Magazine Awards Finalist for Best Multi- and Second-Factor Solution and is a 2010 Network Products Guide Product Innovation Award winner. The company was also recognized with two Gartner reports, Cool Vendors in Identity & Access Management and Cool Vendors in Healthcare Providers'. PhoneFactor has been named to the Bank Technology News FutureNow list of the top 10 technology innovators securing the banking industry today and recently earned a prestigious five stars in the SC Magazine multi-factor authentication group test.

For more information, contact PhoneFactor at **877.No.Token (877.668.6536)** or visit our website at **www.phonefactor.com**.

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 6

PhoneFactor: Phone-Based Two-Factor
Authentication

PhoneFactor Whitepaper

PhoneFactor: Phone-Based Two-Factor Authentication



PhoneFactor, Inc.
7301 West 129th Street
Overland Park, KS 66213
1-877-668-6536
www.phonefactor.com

Executive Summary

Securing access to sensitive corporate and customer data is critical, especially in industries that require a regulatory-compliant environment. Given today's threat landscape, applying usernames and passwords for authentication is insufficient. While two-factor authentication is an effective security solution, traditional methods like security tokens have been difficult to implement, administer, and use. In addition, more sophisticated threats have emerged that redefine established security best practices.

PhoneFactor's two-factor authentication solution leverages an everyday tool – the phone – to secure account logins and transactions. PhoneFactor offers three easy methods - phone call, text message, and phone app - all with the same level of out-of-band security. Users can choose the method that works best for them. PhoneFactor provides maximum flexibility for users and a single platform for IT to manage.

Because there are no devices to deploy, PhoneFactor can be rapidly and economically enabled for large scale enterprise and consumer applications. This paper introduces PhoneFactor phone-based authentication, including how PhoneFactor works, how it is implemented, and how it compares to other two-factor solutions.

Contents

Introduction to Two-Factor Authentication	3
PhoneFactor Overview	4
PhoneFactor Implementation	5
PhoneFactor Security	6
Comparing Two-Factor Systems	7
Conclusion	9

Introduction to Two-Factor Authentication

Authentication, which is the process by which a computer system positively identifies a user, is considered to be one of the weakest links in computer security today. Every day a new story emerges about a computer breach or incident of online fraud resulting from compromised credentials. With the proliferation of remote access and cloud computing among enterprises and increased use of e-commerce and online banking, the trend is only going to continue. Authentication systems that rely solely on user names and passwords are subject to a number of vulnerabilities, including notoriously poor user password choices, password harvesting via key logging software, phishing and man-in-the-middle attacks, and others.

Two-factor authentication adds a critical second layer of security to user logins and transactions. It works by requiring any two of the following:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated)
- Something you are (biometrics)

The security of two-factor authentication lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the trusted device. Conversely, if the user happens to lose the device, the finder of that device won't be able to use it unless he or she also knows the user's password.

Security professionals have deployed various two-factor solutions, but no solution has widely displaced traditional username and password authentication. The industry has seen enterprise deployments of token-based systems from vendors such as RSA® and VeriSign® and smartcard-based solutions. Each solution has significant drawbacks, historically leading to limited adoption by users. For online consumer logins, such as banking and e-government websites, these factors have dramatically limited two-factor deployments. Many banking websites have instead opted to deploy security questions and device identification as an additional layer of security, which are easily circumvented by hackers.

PhoneFactor Overview

PhoneFactor leverages the user's telephone as the trusted device for a second factor of authentication. Telephones are extremely difficult to duplicate and phone numbers are extremely difficult to intercept. The combination of the phone and a username/password yields strong, two-factor authentication with minimal impact on the user experience. And by utilizing an out-of-band channel (the telephone network) for the second authentication, the user is protected against malware on the PC that can be used to log keystrokes and initiate man-in-the-middle attacks.

With PhoneFactor, the user simply logs in with a username and password as normal. Instantly the user's phone rings. The user answers and presses # (or enters a PIN) on the phone keypad to complete the login. The entire process takes just seconds. PhoneFactor also offers SMS authentication in which the user replies to a text message from PhoneFactor to authenticate, and a phone app, which pushes authentication requests to the PhoneFactor App on the user's mobile device. For the maximum level of security utilizing all three authentication factors, the user speaks a secret passphrase during the phone call to also verify their voiceprint.

PhoneFactor is the only two-factor authentication system that allows for instant attack detection. Every authentication attempt in which the attacker knows the user's username and password will generate a phone call, text message, or app notification to the (true) user's phone. That user can immediately block the account and notify the company's fraud department, who can instantly take appropriate action.

PhoneFactor does not require any changes to the user interface and there are no extra devices for users to carry, so little end user training is required. The phone is an inherently user-friendly device and is accessible for users with disabilities. The same phone number can be used to authenticate any application, eliminating the need for multiple devices, and works anywhere in the world. If a user loses or damages their phone, a replacement device can be purchased from a local retailer.

Because there are no security tokens or other devices to deploy or manage and no software or certificates for end users to install, PhoneFactor requires very little effort to implement and virtually no ongoing support. PhoneFactor offers instant integration with all leading business systems

and synchronizes with AD and LDAP servers for centralized user management. Easy, automated self-service options are available through the phone and web, which help to significantly minimize overhead.

PhoneFactor Implementation

PhoneFactor offers instant integration with all leading enterprise applications and seamlessly integrates with existing websites and online transaction processes. Self-enrollment and management tools streamline user deployment and support.

Agent

The PhoneFactor Agent runs within the corporate network. It includes a configuration wizard that guides administrators through the set up process for any applications secured with PhoneFactor, including remote access VPNs, Outlook Web Access, Citrix, IBM Tivoli, and more. Integration with custom applications is also available using the PhoneFactor Web Services SDK or Universal Web Gateway.

Administrators can manage users, configure authentication settings, and check the status of other agents on the network using this simple tool. The Agent can also integrate with existing Active Directory or LDAP servers for centralized user provisioning and management. Redundant synchronized Agents ensure high availability and fail over. All user data is stored within the corporate network for additional security. Extensive logging is available for reporting and auditing.

Direct SDK

Instead of using the Agent to secure applications and manage users, the PhoneFactor Direct SDK offers integration with virtually any web application, and includes web plug-ins for .NET, Java, PHP, Ruby, and Perl, among others. The Direct SDK can be used to integrate into a website's existing login or transaction processes and leverages the site's existing user database.

User Portal

The User Portal is installed within the corporate network and allows users to complete the PhoneFactor enrollment process and manage user settings, such as phone number and PIN, through a simple web interface. Administrative capabilities are also available enabling help desk staff to provide user support.

Online Management Portal

The web-based management portal allows administrators to manage company-wide settings and view centralized usage reports. A robust reporting engine provides detailed and summary views of usage patterns. Reports can be scheduled and emailed directly to IT administrators.

PhoneFactor Service

The PhoneFactor Agent or SDK adds a second step to existing authentication processes. If the username and password are correct, an SSL request is sent to the PhoneFactor Service, which is housed in one of PhoneFactor's data centers around the world. The PhoneFactor Service places a phone call, sends a text message, or pushes a notification to the PhoneFactor App on the user's mobile device and processes the results. Finally, it returns success or failure to the application.

The PhoneFactor Service is supported by a network of redundant data centers and telecommunications providers ensuring the highest level of availability.

PhoneFactor Security

PhoneFactor was developed from the ground up using the latest in secure software design methodologies. The entire system includes strong, mutual authentication, and all network communications are encrypted using high-strength cryptography algorithms. Industry-accepted cryptographic standards are used at every point in the design: authentication is based on X.509 certificates (both client and server), data transport is done using SSL or secure RPC (the same protocol used among domain controllers in Windows networks), and secure resources such as certificates and keys are stored using secure storage providers built into the operating system. Cryptographic-quality random numbers are used whenever randomness is needed.

The data architecture of PhoneFactor is designed to put administrators in total control of their authentication information. All per-user data is stored on the customer site, including the list of users enabled for PhoneFactor. The only information that is passed to PhoneFactor during an authentication is the minimum necessary for appropriate auditing and for the placement of the secondary authentication call or text message.

Administration of the system can be delegated to others via the Phone-Factor User Portal, allowing clean sharing of management responsibilities while retaining a complete audit trail.

Comparing Two-Factor Systems

Two-factor systems have been on the market for years, and the basic concepts have been refined over that time such that the security of two-factor has been well established. However, use of legacy two-factor systems, such as One-Time-Passcodes (OTP), has shifted in recent years to phone-based approaches that offer significant improvements in convenience and security.

One-Time-Passcode (OTP) methods are based on a hardware token, referred to as a security token or OTP token, that generates a pseudo-random sequence of digits that is entered by the user during login. The most popular of these systems is RSA Data Security's SecurID® system. While these systems provide an additional level of security over single-factor authentication systems, they have proven to be cumbersome for IT departments and end users.

Security tokens do not protect against current threats, such as man-in-the-middle/browser attacks and other modern forms of malware. As the sophistication of attacks continues to increase, out-of-band authentication, which utilizes a separate channel for the second factor of authentication, is becoming widely recognized as a best practice for two-factor authentication. Any method, such as a security token or fob, usb token, and even soft tokens, which require an OTP be keyed into the original login interface, do not meet the criteria for out-of-band authentication and as such are vulnerable to attack.

In addition, users are resistant to carrying an extra device, and as more companies implement two-factor authentication, users could be required to carry multiple security tokens – one for their online bank account, one for their trading account, and one for their corporate vpn. Security tokens are easy to lose or break, creating a frustrating experience for users and placing a large burden on your IT department.

Because token-based systems require users to change their behavior substantially, significant training is needed. Users sometimes have a hard time

remembering which order the PIN and the token passcode are entered, and training users to “wait for the bars” is difficult. Some systems even require administrators to modify applications before they will work, invoking all of the change control difficulties associated with non-standard vendor software.

Since security tokens must be provisioned, mailed, inventoried and replaced, they require significant IT resources to deploy and support. Security tokens are lost at a rate of up to 10% each year, expiring tokens must be re-provisioned every 2-5 years, and tokens can get out of sync, meaning the OTP that is generated is not the same one the login application is expecting. The resulting costs to an IT department can become a material part of the total cost of ownership for a token solution.

Software tokens do not require a physical device be deployed to users, so hard costs are less than hardware security tokens. However the same security and usability issues that apply to hardware tokens also apply to their software counterparts.

Another common two-factor solution involves the use of smartcards. Smartcards are credit card-sized tokens that have an embedded private key that is protected by a PIN or password. This private key positively identifies the user to the system. Like tokens, users are required to carry around a new object that they didn't have before. Cards must be provisioned, mailed, inventoried and replaced, creating similar logistical problems. And, since very few computers have built-in smartcard readers, an additional piece of hardware, together with drivers (and associated platform dependencies), must be distributed and installed by users. This creates a single channel of communication, making it vulnerable to man-in-the-middle/browser attacks. Smartcards present lockout risks – most cards deactivate themselves after a certain number of failed attempts, and require physical replacement. Finally, few applications have native support for smartcard technology, and those that do often have narrow support for operating system versions, card reader models, and so on.

Unlike security tokens and smartcards, PhoneFactor combines the high degree of security companies need to protect against today's attacks with a solution that is easy to set up, maintain, and use. Because users already have phones, there is no hardware distribution. If a user's phone is lost, that user has the responsibility of replacing it, not the company. All that is required for provisioning is getting users' phone numbers, and often that

data is already available in a company directory, with which PhoneFactor can easily integrate. PhoneFactor doesn't require application-specific changes, making it compatible with a broad range of applications. It uses standard, documented interfaces to add the secondary authentication step, thereby helping to ensure future compatibility. User training is simple, typically accomplished with an automated welcome email, and customizable prompts guide the user through the authentication process. There are never synchronization or lock-out issues, and the user's computer needs no extra hardware or drivers.

Conclusion

Username and passwords no longer provide adequate security. As escalating threats and strengthening regulatory requirements drive increased adoption of two-factor authentication, companies are increasingly looking to PhoneFactor's phone-based authentication solutions to provide the strong security needed to protect against today's threats without burdening users or IT departments.

PhoneFactor is trusted by thousands of organizations across virtually every industry, including Retail, Government, Health Care, and Banking, to secure millions of logins and online transactions each month.

PhoneFactor was recognized in 2011, 2010, and 2008 as an SC Magazine Awards Finalist for Best Multi- and Second-Factor Solution and is a 2010 Network Products Guide Product Innovation Award winner. The company was also recognized with two Gartner reports, Cool Vendors in Identity & Access Management and Cool Vendors in Healthcare Providers'. PhoneFactor has been named to the Bank Technology News FutureNow list of the top 10 technology innovators securing the banking industry today and recently earned a prestigious five stars in the SC Magazine multi-factor authentication group test.

For more information, contact PhoneFactor at **877.No.Token (877.668.6536)** or visit our website at **www.phonefactor.com**.

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 7

Section 7 – PhoneFactor SMS (Text)
Authentication Datasheet

<http://www.phonefactor.com/products/sms-text-authentication>



PhoneFactor

[Free Download](#)

[Resource Center](#)

[Customer Login](#)

1.877.No.Token (1.877.668.6536)

[Live Chat](#)

[Online Demo](#)

[Free Download](#)

[Solutions](#)

[Products](#)

[How It Works](#)

[Company](#)

SMS (Text) Authentication

Add PhoneFactor's SMS Authentication to the Extended Edition to allow users to choose the authentication method they prefer, phone call or SMS text message, all with the same level of out-of-band security and convenience.

PhoneFactor SMS Authentication Offers:

- 100% Out-of-Band Authentication or Standard OTP Authentication
- PIN Security
- Support for Transaction Verification
- Flexibility for End Users and Simplicity for IT

Key Features

100% Out-of-Band Authentication

Instead of placing a voice call to the user, PhoneFactor SMS Authentication sends a one-time passcode to the user's mobile phone via an SMS text message. The user sends a text message reply that contains the one-time passcode to authenticate. Because the one-time passcode is both sent and confirmed through SMS, the process is completely out-of-band.

Standard OTP Authentication

Instead of replying to the SMS text message, organizations can allow users to enter the one-time passcode directly into the login interface. As with a security token, the user must enter a one-time passcode to verify the possession of a trusted device. But unlike tokens, PhoneFactor leverages a device the user already has – their phone.

PIN Security

Add a third layer of protection by requiring users to provide a personal identification number (PIN) in addition to the one-time passcode to authenticate.

User Choice

Configure all users for SMS Authentication or allow users to choose between a voice call and SMS text message for authenticating. Users simply choose a method during enrollment or at any time from the User Portal. This enables the ultimate flexibility for your users and a single platform for your IT team to manage.

Custom Messages

Customize the PhoneFactor experience for your users. Increase usability with SMS text messages specific to your company and home language, and customize the automated welcome e-mail that is sent to users.

Support for Transaction Verification

Details about transactions can be provided in the SMS text message. So, even if the user's authenticated session has been hijacked, the attacker cannot complete a transaction without the user's explicit approval.

Robust, Scalable Authentication Platform

SMS Authentication is available as an add-on to the PhoneFactor Extended Edition, which include support for directory synchronization, user self-service, redundancy, and robust reporting and logging capabilities.



Demo PhoneFactor

See for yourself
how easy it is.



Get PhoneFactor

It's Free

Sign up now to get started.



Contact Us

Call **877.No.Token**

Or click to **Chat Live**

Products

PhoneFactor Free

PhoneFactor Standard

PhoneFactor Extended

SMS Text Authentication

Biometric Authentication

Transaction Verification

Phone Verification

Global Services

24/7 Support

PhoneFactor
Infringement Chart
(6,934,858 and 7,574,733)
Reference Documents

Section 8

Section 8 – Comparing PhoneFactor to Other
SMS Authentication Solutions Datasheet

<http://www.phonefactor.com/sms-authentication>



PhoneFactor

[Free Download](#)
[Resource Center](#)
[Customer Login](#)
1.877.No.Token (1.877.668.6536)

[Live Chat](#)
[Online Demo](#)
[Free Download](#)
[Solutions](#)
[Products](#)
[How It Works](#)
[Company](#)

Comparing PhoneFactor to Other SMS Authentication Solutions

Evaluating two-factor authentication solutions requires a look at three critical areas – the security and scalability of the technology, hurdles to user adoption, and the total cost (including internal costs) to deploy and support the system. Below is an analysis of the sms two-factor authentication systems on the market today and PhoneFactor's authentication solution, which includes support for authentication via an automated voice call, SMS text message, and phone app.

Other SMS Authentication Solutions

With other **SMS authentication systems**, a One-Time Password (OTP) is sent to the user via a text message to their cell phone. As with a security token, the user must enter the OTP into the login interface to verify the possession of a trusted device. But unlike tokens, SMS authentication systems leverage a device the user already has – their cell phone. There are some 3.5 billion cell phones in the world today, which is a big advantage over tokens and other security devices.

However, one of the biggest disadvantages of most **SMS authentication solutions** is that they do not protect against emerging threats, such as man-in-the-middle attacks. As the sophistication of attacks continues to increase, Out-of-Band authentication, which utilizes a separate channel for the second factor of authentication, is becoming widely recognized as a best practice for two-factor authentication. Any authentication method that requires a OTP be keyed into the original login interface does not meet the criteria for out-of-band authentication and as such is vulnerable to attack.

PhoneFactor Out-of-Band Authentication

PhoneFactor also leverages the phone for two-factor authentication and provide authentication through an SMS text message, as well as an automated voice call and smartphone app, but with some important differences from other **SMS authentication** providers. With PhoneFactor, users simply login with their username and password – just like they do today. Instantly an SMS text message with a One-Time Password is sent to the user. The user simply replies to the SMS message with the OTP to authenticate. Because the One-Time Password is both sent and confirmed through an SMS text message, the process is completely out-of-band.

By combining out-of-band authentication with real-time fraud alerts, PhoneFactor offers the strongest level of security on the market today. The PhoneFactor platform relies exclusively on the telephone network for the second factor of authentication which ensures protection against keystroke loggers and man-in-the-middle attacks. PhoneFactor can be used to verify specific high-risk transactions, so even if the user's authenticated session has been hijacked, their transactions are protected. Not only does PhoneFactor prevent unauthorized logins and transactions, it notifies you instantly if a user's credentials have been compromised and an attack is in progress. Security tokens are simply not capable of alerting you to an attack.

PhoneFactor requires very little effort to implement and virtually no ongoing support. PhoneFactor offers instant integration with all leading business systems and synchronizes with AD and LDAP Servers for centralized user management. Easy, automated self-service options are available through the phone and web, which helps to significantly minimize overhead. It is easy to use, requiring no end user training.

Technology

- Out-of-band authentication with live fraud alerts
- Instant integration with leading enterprise systems
- Web plug-ins integrate with existing websites and online transaction processes
- User enrollment and self-service tools keep overhead low

User Adoption

- Flexible user options – phone call, text message, and phone app
- No changes to the user login experience


Demo PhoneFactor

 See for yourself
how easy it is.


Get PhoneFactor

It's Free

Sign up now to get started.



Contact Us

 Call **877.No.Token**

 Or click to **Chat Live**
[Compare SMS
Authentication Solutions](#)

Low annual fee per user or per auth

Cost

- No hardware to purchase or install

PhoneFactor’s two-factor authentication service with phone and sms authentication options offers a greater level of security than other *SMS authentication* providers. And because PhoneFactor allows users to choose the authentication method they prefer (phone call or SMS text message), it enables the ultimate flexibility for your users and a single platform for your IT team to manage. For more information on PhoneFactor’s sms authentication try the [PhoneFactor Demo](#) or [Download the Free Version](#).

© 2007-2012 PhoneFactor, Inc. [Terms](#) | [Sitemap](#) | [Support](#) | [Contact](#)



PhoneFactor, Inc provides secure two-factor authentication services to leading companies worldwide. PhoneFactor's multifactor out-of-band authentication software is a cost effective, user friendly alternative to security tokens, fobs, certificates, and other 2 factor authentication methods.

Secure User Authentication: [SSL VPN Authentication](#) | [Citrix Authentication](#) | [Web Authentication](#) | [Terminal Services Authentication](#) | [Tivoli Authentication](#) | [Online Banking Authentication](#)

Two-Factor Authentication for Regulatory Compliance: [Payment Card Industry Data Security Standards \(PCI DSS\) Compliance](#) | [FFIEC Compliance](#) | [HIPAA Compliance](#) | [NIST 800-63](#)

Compare Phone Authentication to: [Security Tokens](#) | [SMS Authentication](#) | [Biometric Authentication](#) | [Soft Tokens](#) | [Smart Cards](#) | [Certificates](#)